UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/822,220	04/09/2004	Semyon B. Mizikovsky	2100.006100	1318

7590 04/28/2008

Terry D. Morgan
Williams, Morgan & Amerson, P.C.
Suite 1100
10333 Richmond
Houston, TX 77042

EXAMINER	
OKORONKWO, CHINWENDU C	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
04/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/822,220	MIZIKOVSKY, SEMYON B.	
	Examiner	Art Unit	
	CHINWENDU C. OKORONKWO	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 February 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. In response to communications filed on 02/07/2008, the Examiner acknowledges the amendments made to the claims and have both considered and applied them to the claims.

In response to communications filed on 02/07/2008, applicant amends claims 1, 4 and 8. The following claims, claims 1-11 are presented for examination.

Response to Remarks/Arguments

1.1 Applicant's arguments, with respect to the rejection of claims 1-11 have been fully considered but they are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malinen et al. (U.S. Patent Application Publication No. 2005/0078824 A1) in view

of Quick ("Common Security Algorithms" - 3rd Generation Partnership Project 2. Qualcomm Incorporated, July 10, 2002,).

Regarding claims 1 and 11, Malinen et al., discloses a method, comprising: receiving a first challenge associated with a first authentication process (0075 – "On receiving the message the AS first identifies the AuC holding the authentication information for the user. (this first identification is equated to the first authentication" and "[Access Server (AS)] creates the Extensible Access protocol (EAP) Request/AKA/Challenge message containing the AT_RAND value, the AT_AUTN value, and the AT_MAC value") is equated to the first challenge; deriving a second challenge associated with a second authentication process based on at least a portion of the first challenge (0075 – "[Access Server (AS) creates and] sends a message, containing the EAP Request/AKA/Challenge message in it and the NAI identifying the user (in the User-Name attribute), to the AC.") is equated to the second challenge; performing the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom (0077 – "When the terminal receives this message, it first extracts the EAP Request/AKA/Challenge message. It then uses the AKA to calculate the AT_RES values, giving the AT_RAND and AT_MAC values received inside the EAP Request/AKA/Challenge as input to the AKA. It also calculates the AT_AUTN value and compares it to the AT_AUTN received in the EAP

Request/AKA/Challenge. If these values match, the EAP Request/AKA/Challenge message is authenticated successfully.");
a key associated with the first authentication process based on the at least one authentication parameter (0056 – "Several authentication mechanisms may be used. In the following description of the preferred embodiments, EAP-AKA (Authentication and Key Agreement) authentication mechanism using USIM (Universal Subscriber Identity Module) (first embodiment) and an authentication mechanism using R-UIM (removable user identity module) applying a CAVE (Cellular Authentication and Voice Encryption) algorithm (second embodiment) are taken as examples").

Malinen et al. is silent in disclosing performing an authentication using the RAND challenge to produce a SMEKEY and a PLCM (0152-0154 and 0147-0157); and deriving a secret CHAP key based on the SMEKEY and PLCM., however Malinen et al. does disclose "an authentication mechanism using … a Cellular Authentication and Voice Encryption (CAVE) algorithm, or a USIM applying te AKA algorithm (0030-0031)," this disclosure in combination with the Quick disclosure of, creating "the CDMA private long code mask (PLCM) and the message encryption key CMEAKEY for intersystem handoff from a system using AKA to a system using older (2G) algorithms for authentication and privacy. (On the ANS-41 network, these keys are referred to as CDMA_PLCM and SMEKEY.) "(Quick page 9). It would have been obvious for one of ordinary skill in the art to

have modified the disclosed CDMA private long code mask (PLCM) and the message encryption key CMEAKEY of Quick into the SMEKEY and PLCM of the instant application because these terminologies are used interchangeably.

Regarding claim 2, Malinen et al., discloses a method, as set forth in claim 1, wherein receiving the first challenge associated with the first authentication process further comprises receiving a CHAP challenge (0152 – "packet data sessions via a PDSN, as is currently done with EAP-CHAP").

Regarding claim 3, Malinen et al., discloses a method, as set forth in claim 2, wherein deriving the second challenge associated with the second authentication process based on at least a portion of the first challenge further comprises deriving a RAND challenge based on at least a portion of the CHAP challenge ("[Access Server (AS)] creates the Extensible Access protocol (EAP) Request/AKA/Challenge message containing the AT_RAND value, the AT_AUTN value, and the AT_MAC value") is equated to the first challenge and "a message, containing the EAP Request/AKA/Challenge message in it and the NAI identifying the user (in the User-Name attribute), to the AC.") is equated to the second challenge).

Regarding claim 4, Malinen et al., discloses a method, as set forth in claim 3, wherein deriving the RAND challenge based on at least a portion of the CHAP

challenge further comprises deriving the RAND challenge by concatenating the CHAP challenge (0152-0154).

Regarding claim 5, Malinen et al., discloses a method, as set forth in claim 4, wherein performing the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom further comprises performing a CAVE based authentication process on the RAND challenge to produce SMEKEY (0030, 0056, 0144-146 and rejected the same rationale as claim 1).

Regarding claim 6, Malinen et al., discloses a method, as set forth in claim 5 wherein performing the CAVE based authentication process on the RAND challenge to produce SMEKEY further comprises performing the CAVE based authentication process on the RAND challenge to produce SMEKEY and PLCM. (Rejected under the same rationale as claim 1).

Regarding claim 7, Malinen et al., discloses a method, as set forth in claim 6, wherein deriving the key associated with the first authentication process based on the at least one authentication parameter further comprises deriving the key associated with the first authentication process based on SMEKEY and PLCM (Rejected under the same rationale as claim 1).

Regarding claim 8, Malinen et al., discloses a method, as set forth in claim 1, further comprising delivering the key to a network to request access to the network (0056-0060).

Regarding claim 9, Malinen et al., discloses a method, as set forth in claim 8, further comprising: determining that the first challenge associated with the first authentication process is a re-authentication challenge (0073-0074); bypassing the derivation of the second challenge associated with the second authentication process based on at least a portion of the first challenge in response to the determining that the first challenge is the re-authentication challenge (0075); bypassing the performance of the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom in response to the determining that the first challenge is the re-authentication challenge (0076-0079).

Malinen et al. is silent in disclosing the key associated with the first authentication process based on the at least one authentication parameter further comprises using a previously derived key in response to the determining that the first challenge is the re-authentication challenge (0056-0060 of Malinen et al.).

Regarding claim 10, Malinen et al., discloses a method, as set forth in claim 8, further comprising: determining that the first challenge associated with the first authentication process is a re-authentication challenge (0073-0074); and wherein delivering the key to a network to request access to the network further comprises delivering a previously derived key in response to the determining that the first challenge is the re-authentication challenge (0076-0079).

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 9:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. C. O./

Examiner, Art Unit 2136

April 24, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136